



Executive Institute Presents
California CIO Forum - Friday April 16, 2004

“Closing the Loop on Enterprise Operations & Security: *A Silver Bullet at Last?*”

Tom Jones, Chief Information Security Officer
Health & Human Services Data Center (HHSDC)
tjones1@hhsdc.ca.gov



August 11, 2003???

RPC DCOM (ports 135, 137, 138, 139, 445)

Blaster, LoveSan, Welchia, Nachi



Closed-Loop Enterprise System Maintenance (ESM)

“A Practical Look”

Closed-Loop Enterprise System Maintenance (ESM)

A. Assumptions

- 1. Can scale from a single site to Enterprise-level deployment(s)**
- 2. All processes automated with appropriate human interventions**
- 3. Components can be from a single vendor or multiple vendors, but all must be integrated using a common infrastructure**

B. Components

1. Asset Management

- a. Must support all of our OSs/HW/SW**
- b. Must be agent-based**
- c. Agents must be nimble, efficient and highly configurable scanning options**
- d. Must perform equally well in both a centralized and decentralized environment**
- e. Required synchronizations must be seamless and failsafe**
- f. Must contain extensive reporting capabilities**
- g. Must be integrated with VA Scanning Tools (Nessus, nCircle, etc.)**

2. Integrated Alert/Threat Management System

- a. Accurate, detailed, technology-specific notifications provided on a timely basis**
- b. Sourced from worldwide sensor data**
- c. Accurate, appropriate threat mitigation strategies and prioritizations**
- d. Must be integrated into Patch Management/Triage/Scheduling System**

3. Patch Management/Triage/Scheduling System

- a. Integrated to drive workload based on Risk Assessment rules and protocols**

4. Software Distribution

- a. Integrated to existing change management process**
- b. Controlled rollout (Test/Production)**
- c. Rollback capability**
- d. Comprehensive Scheduling**
- e. Compliance enforcement**
- f. Dependencies verification**
- g. Feedback to central or distributed repositories.**

Vulnerability Management

Vulnerability Assessment/Scanning, Configuration Management, and Patch Distribution / Management markets expected to be absorbed into an overarching Vulnerability Management market space.

By 2007, the patch management feature set is expected to be absorbed and disappear into other markets such as the desktop and server management, vulnerability management and security management suites.*



* Source: Gartner "Market Analysis: Patch Management is a Fast Growing Market", May 2003.

Security Patch - Best Practices



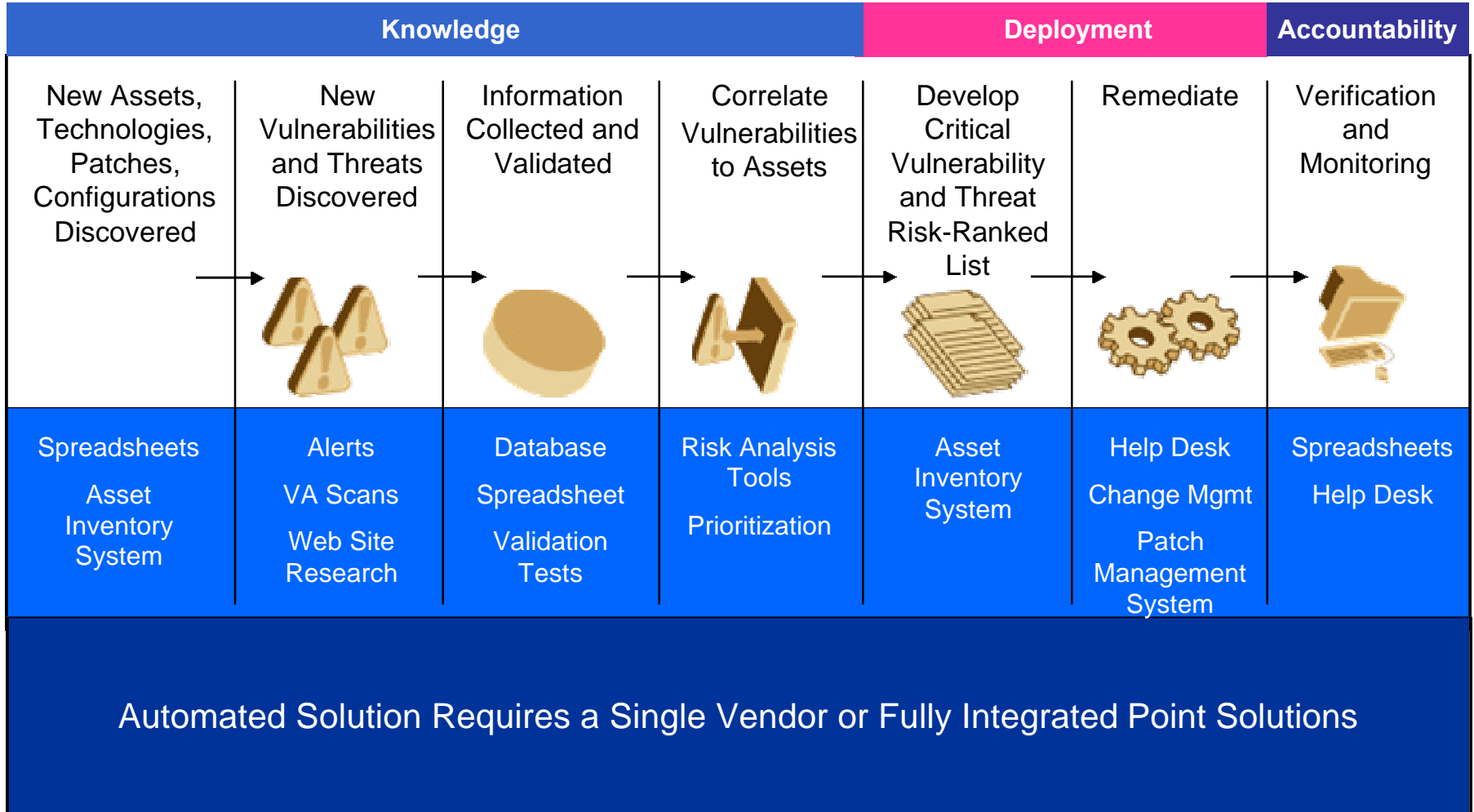
**National Institute of
Standards and Technology**

1. Creating an automated organizational hardware and software inventory, augmented with periodic vulnerability scans
2. Identifying newly discovered vulnerabilities and security patches
3. Prioritizing patch application
4. Creating an organization-specific patch database
5. Testing patches for functionality and security (to the degree that resources allow)
6. Distributing patch and vulnerability information to local administrators
7. Verifying patch installation through network and host vulnerability scanning
8. Training system administrators in the use of vulnerability databases
9. Deploying patches automatically (when applicable)
10. Configure automatic update of applications (when applicable)

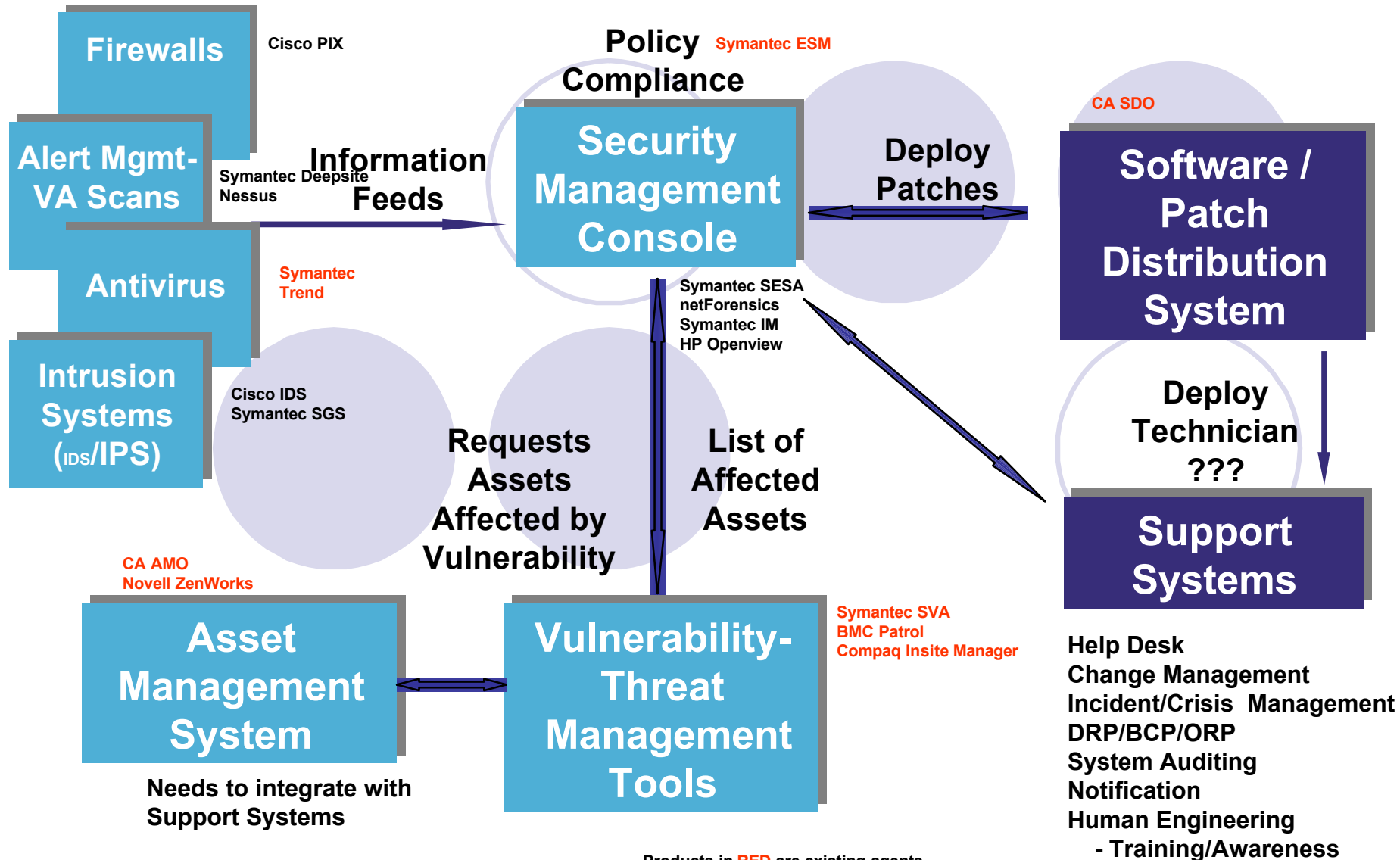
4 Pillars to Vulnerability Management

- Know *what you have*
 - Know your network assets and what software is loaded
- Know the *exposures*
 - Know what threats affect each individual asset and know how risky each threat is
- Know what *action to take*
 - Have the information and the method to quickly and easily fix systems
- Be able to *measure status and progress*
 - Have a method of measuring work and summarizing risks in reports

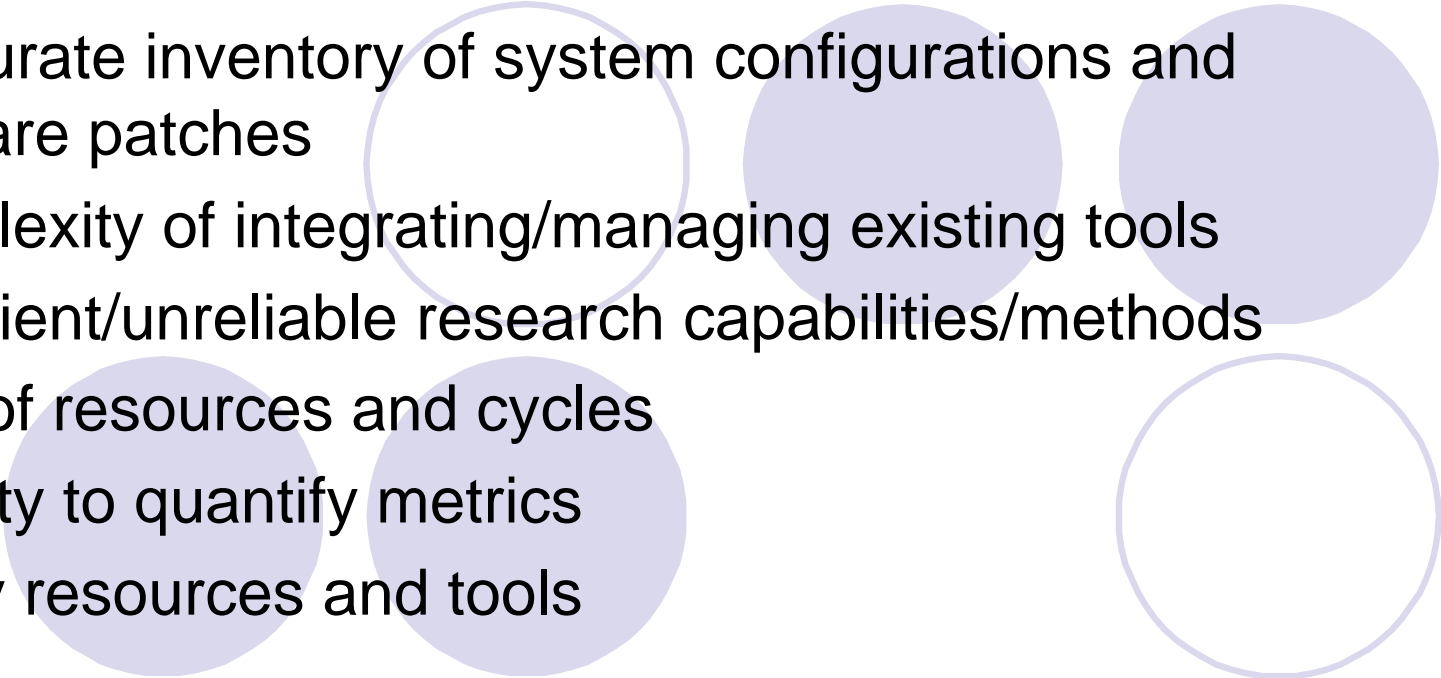
Vulnerability Management Process



Vulnerability Management



Vulnerability Management Obstacles

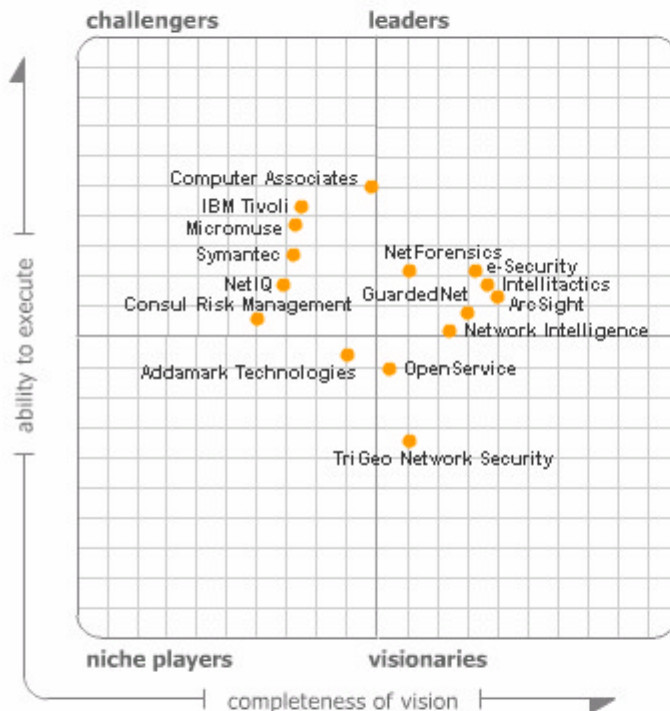
- Inaccurate inventory of system configurations and software patches
 - Complexity of integrating/managing existing tools
 - Inefficient/unreliable research capabilities/methods
 - Lack of resources and cycles
 - Inability to quantify metrics
 - Costly resources and tools
- 

Magic Quadrant for IT Security Management, 1H04

Author: [Mark Nicolett](#)

Date: 26 March 2003

Note #: M-21-9150

[? Help](#)
[Read the Full Report](#)
[Print Version \(pdf\)](#)
[Market Overview](#)
[Vendor Criteria](#)
[Quadrants](#)
[Ability to Execute](#)
[Completeness of Vision](#)


Market Overview

About This Market

The IT security management market is driven by enterprises' needs to filter, aggregate and correlate security data from heterogeneous sources for real-time monitoring and historical analysis. Primary adopters of this technology tend to be large organizations with a complex IT infrastructure and dedicated IT security staff. Leaders are driving the market in terms of technical innovation, have rapidly growing production installed bases, and frequently are selected for and win competitive evaluations by organizations that make product-selection decisions based primarily on IT security management requirements.

Recommended Reading

Research:

[IT Security Management Technology Evaluation, 1H04](#)

[IT Security Management Broad-Scope Software Vendors, 1H04](#)

[IT Security Management Point Solution Vendors, 1H04](#)

[update preferences](#)

© 2004 Gartner, Inc. and/or its Affiliates. All Rights Reserved.